http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.23, No.3, August 2018, pp.129-143
https://doi.org/10.7838/jsebs.2018.23.3.129

정보저장매체 반출 및 디지털 증거탐색 과정에서의 참여권 보장 환경에 대한 중요도-이행도 분석

Enabling Environment for Participation in Information Storage Media Export and Digital Evidence Search Process using IPA

양상희(Sang Hee Yang)*, 이중정(Choong C. Lee)**, 윤혜정(Haejung Yun)***

초 록

최근 컴퓨터, 스마트 기기 등 디지털 매체의 사용이 급격히 늘어나면서, 이들 기기에 저장되는 정보 또한 방대하고 다양한 방식으로 저장되고 있다. 이들 정보는 수사기관의 영장에 기재된 범죄와 무관한 정보, 즉 별건 정보도 포함하고 있으므로, 이를 압수수색 할 경우 피압수자의 기본권과 방어권, 사생활 침해가 우려된다. 최근 들어 정보저장매체 등의 압수수색 절차에서 피압수자 참여권의 중요성을 강조함으로써 참여권에 대한 관심이 커지고 있다. 이에 각 수사 기관은 참여권을 보장하기 위해 노력하고 있으나 구체적인 가이드라인이 없는 상태로 상황과 환경에 따라 각기 다른 방식으로 시행하고 있다. 이 과정에서 피압수자 측의 참여권 보장 악용으로 수사의 신속성・보안성이 저하되거나, 참여 시 원격초기화 등을 통한 증거인멸까지 시도되는 부작용이 발생하고 있다. 본 연구에서는 정보저장매체의 현장 외 반출 및 디지털 증거탐색 과정에서의 참여권 보장 환경에 대하여 4개 상위 영역과 30개 하위 측정 항목으로 전국의 디지털 증거분석관을 대상으로 설문조사를 실시하였다. 중요도 수준과 이행도 수준의 차이를 IPA 매트릭스 분석기법을 통해 절차, 장소, 사람, 기술요인 평가로 나누어 분석 하였다. 중점개선영역에 속한 7개 항목은 절차 항목 1개, 장소 항목 3개, 사람 항목 3개로 나타났다. 우선적인 지원 및 개선 사항이 요구되는 항목에 대한 피압수자의 기본권, 방어권, 사생활 침해에 대한 권리 보장과 부작용 사례를 최소화하고, 디지털 증거분석관의 신속도, 효율성을 저하시키지 않는 참여권 보장 환경을 만들기 위한 유용한 근거로 활용 되는 것에 본 연구의 의의가 있다.

ABSTRACT

Recently, the use of digital media such as computers and smart devices has been rapidly increasing, The vast and diverse information contained in the warrant of the investigating agency also includes the one irrelevant to the crime. Therefore, when confiscating the information, the basic rights, defense rights and privacy invasion of the person to be seized

* Graduate School of Information, Yonsei University(cyberyang@police.go.kr)
** Graduate School of Information, Yonsei University(cclee@yonsei.ac.kr)
*** Corresponding Author, College of Science & Industry Convergence, Ewha Womans University (yunhj@ewha.ac.kr)
Received: 2018-06-21, Review completed: 2018-07-05, Accepted: 2018-07-16

have been the center of criticism. Although the investigation agency guarantees the right to participate, it does not have specific guidelines, so they are various by the contexts and environments. In this process, the abuse of the participation right is detrimental to the speed and integrity of the investigation, and there is a side effect that the digital evidence might be destroyed by remote initialization. In this study, we conducted surveys of digital evidence analysts across the country based on four domains and thirty measurement items for enabling environment for participation in information storage media export and digital evidence search process. The difference between the level of importance and the performance was analyzed by the IPA matrix based on process, location, people, and technology dimensions. Seven items belonging to “concentrate here” area are one process-related, three location-related, and three people-related items. This study is meaningful to be a basis for establishing the proper policies and strategies for ensuring participation right, as well as for minimizing the side effects.

키워드 : 정보저장매체 반출, 디지털 증거, 디지털 포렌식, 참여권 보장, 중요도-이행도 분석(IPA)
Information Storage Media Export, Digital Evidence, Digital Forensic, Participation, IPA

1. 서 론

최근 컴퓨터와 스마트폰 등 디지털 매체의 사용이 급격히 늘어나면서, 이러한 기기에 저장되는 정보 또한 방대하고 다양한 방식으로 저장되고 있으며 법적 증거로도 활용되고 있다[7]. 따라서 디지털 기기는 범죄혐의를 찾기 위해 반드시 포함되는 압수수색 대상이 되었고, 디지털 증거분석은 범죄를 수사함에 있어서 수사 절차의 일부로 인식되고, 수사의 성패를 좌우할 정도로 중요한 비중을 차지하게 되었다[4]. 디지털 증거의 중요성이 증가함에 따라 디지털 매체에 대한 증거분석 건수는 2010년 6,247건, 2013년 11,200건, 2016년에는 32,281건에 이를 정도로 급증하고 있다[1].

중요 사건 수사 및 공판과정에서 디지털 증거의 증거능력 내지 압수수색의 적법성 여부가 핵심 쟁점으로 떠오르면서 이와 관련된 법제와 판례들도 급속한 변화를 겪고 있다. 대법원 2015. 7. 16자 2011모1839 전원합의체 결정에서 정보저장매체 등의 압수수색절차의 적법성이 문제가 되었다. 영장에 기재된 범죄와 무관한 정보가 혼재된 상태에서 압수수색현장에서 반출된 정보저장매체를 수사기관 사무실에서 탐색, 출력하는 중에 피압수자 측에 참여 기회를 제공하지 않았기 때문이다. 해당 판례 이후 수사기관에서는 압수수색 시작부터 종료까지 전 과정에서 피압수자의 기본권과 방어권, 사생활 침해를 보호하는 참여권의 중요성이 강조되고 있다[4]. 그러나 구체적 지침이나 제반사항에 대한 규칙이 없고, 참여권 보장으로 인해 발생할 수 있는 문제점들이 우려되고 있는 실정이다[1].

따라서 본 연구에서는 피압수자의 기본권을 보장하고 사생활 침해를 방지하는 참여권 보장의 헌법적 가치를 실행함과 동시에 부작용을 최소화하고 수사의 효율성을 높이기 위해, 압수수색 현장 외로 반출된 정보저장매체의 디지털 증거탐색 시 참여권 보장 환경에 대한 현황 및 인식 연구를 수행하고자 한다. 이를 위해 다음의 <Table 1>과 같이 연구 질문을 설정하였다.

〈Table 1〉 Research Questions

No.	Research Questions
1	What is the difference between importance and performance of enabling environment for participation in information storage media export and digital evidence search process?
2	As a result of IPA, which dimensions and items have the priority for support and improvement?

이를 위하여, 먼저 전문가 회의를 통해 참여권 보장 환경에서 중요하다고 생각하는 상위의 영역과 하위의 측정항목을 도출한다. 다음으로는 각 항목의 중요도와 이행도의 차이를 IPA 매트릭스를 활용하여 분석을 진행한다. 이를 통해 수사기관이 준수해야하는 절차, 갖춰야 하는 장소, 고려해야 하는 사람, 제공해야 하는 기술에 대하여 중점 지원 및 개선되어야 하는 세부항목을 알아본다. 본 연구의 결과는 향후 참여권 보장 관련 가이드라인 또는 규칙 마련의 기초자료로 활용될 수 있을 것이다.

본 논문은 다음과 같이 구성된다. 제 2장에서는 디지털 증거의 참여권 관련 현행 법규와 훈령 등을 알아보고, 참여권 보장 제도의 문제점을 살펴본다. 제 3장에서는 본 연구의 분석 방법인 중요도-이행도 분석(IPA)의 개념을 알아보고, 연구의 절차를 소개한다. 제 4장에서는 사전조사 결과와 IPA 분석 결과를 보고하고, 마지막 제 5장에서는 연구 결과에 따른 시사점에 대해 논의하고 향후 연구 과제를 제안한다.

2. 이론적 배경

2.1 디지털 증거의 참여권 관련 현행 법규

형사소송법에서는 압수・수색 절차에서 피압수자의 참여권을 별도 조문으로 규정하고 있지 않다[2]. 그러나 '제121조(영장집행과 당사자의 참여) 검사, 피고인 또는 변호인은 압수・수색영장의 집행에 참여할 수 있다.' '제122조(영장집행과 참여권자에의 통지) 압수・수색영장을 집행함에는 미리 집행의 일시와 장소를 전조에 규정한 자에게 통지하여야한다. 단, 전조에 규정한자가 참여하지 아니한다는 의사를 명시한 때 또는 급속을 요하는 때는 예외로 한다.' '제118조(영장의 제시) 압수・수색영장은 처분을 받는 자에게 반드시 제시하여야 한다.' '제123조(영장의 집행과 책임자의 참여) ① 공무소, 군사용의 항공기 또는 선차 내에서 압수・수색영장을 집행함에는 그 책임자에게 참여할 것을 통지하여야 한다. ② 전항에 규정한 이외의 타인의 주거, 간수자 있는 가옥, 건조물, 항공기 또는 선차 내에서 압수・수색영장을 집행함에는 주거주, 간수자 또는 이에 준하는 자를 참여하게 하여야 한다. ③ 전항의 자를 참여하게 하지 못할 때에는 인거인 또는 지방공공단체의 직원을 참여하게 하여야 한다.' '제129조(압수목록의 교부) 압수한 경우에는 목록을 작성하여 소유자, 소지자, 보관자 기타 이에 준할 자에게 교부하여야 한다.' '제106조(압수) 제3항 법원은 압수의 목적물이 컴퓨터용 디스크, 그 밖에 이와 비슷한 정보저장매체인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체 등을 압수 할 수 있다.'고

규정하고 있다. 또한 제219조(준용규정)에 따라 이러한 조문을 수사기관의 압수, 수색 또는 검증에 준용하고 있어, 디지털 증거탐색 과정에서 피압수자의 참여권이 인정된다고 볼 수 있다.

2.2 경찰의 디지털 증거 수집 및 처리 등에 관한 규칙(훈령)

현행 경찰청훈령 제845호는 2011모 1839 전원합위체 결정에 따른 '관련성' 있는 정보만 출력・복제하고, 수사기관 등으로 반출하여 출력・복제하는 경우에도 '참여권을 보장'하며, '별건 사건관련 증거' 발견 시 추가 탐색을 중지하는 등 디지털 증거의 압수・수색・검증 절차를 상세히 규정하고 있다. 이와 같이, 단순히 법률과 영장의 기재에 따라야 한다는 기존의 선언적인 규정을 구체화하여 변화된 사법적 요구를 반영하고 있다[6].

개정사항을 살펴보면 첫째, 제11조(디지털 데이터의 압수・수색・검증)에서 '디지털 데이터를 압수하는 경우에는 범죄사실과 관계가 있다고 인정할 수 있는 범위를 정하여 출력하거나 복제하는 방법으로 압수하여야 한다.'라고 규정하고 '제1항의 방법이 불가능하거나 현저히 곤란한 경우에는 복제본을 획득하여 외부로 반출한 후, 제1항의 방법으로 디지털 데이터를 압수할 수 있다.' '제1항 및 제2항의 방법이 불가능하거나 현저히 곤란한 경우에는 디지털 저장매체 원본을 외부로 반출한 후, 제1항 또는 제2항의 방법으로 디지털 데이터를 압수할 수 있다.'라고 명시하고 있다. 위 조항의 본문과 관련하여서는 제11조 4항에서 '디지털 데이터를 압수하는 경우에는 참여인의 참여권을 보장하여야 한다.' 및 제11조 5항에서 '제1항부터 제3항까지의 규정에 따라 디지털 데이터를 압수하는 경우에는 데이터 고유 식별값(이하 "해시값"이라고 한다) 확인 등 디지털 증거의 동일성, 무결성을 담보할 수 있는 적절한 방법과 조치를 취하여야 한다.'라고 규정하여 범죄사실과 관련 있는 디지털 데이터의 현장압수, 참여권 보장, 해시값 확인 등을 현행 영장집행 실무에 반영하였다.

둘째, 제12조(확인서 등)에서 '제11조2항에 따라 획득한 복제본을 반출하는 경우에는 해시값 확인 및 참여권 고지 후 복제본 반출(획득) 확인서를 작성하여야한다.' '제3항 디지털 저장매체 원본을 반출하는 경우에는 원본 봉인 및 참여권 고지 후 원본 반출 확인서를 작성하여야 한다.' '제5항 수사관 또는 증거분석관은 압수・수색・검증 과정에서 피압수자등이 참여를 철회하는 경우에는 참여철회 확인서를 작성하도록 하여야 한다.'라고 명시하여 원본을 압수하는 경우의 참여권 보장과 디지털 증거의 무결성 확보를 위한 압수 절차별 확인 서식을 신설하였다.

셋째, '제13조2항에서 해시값 확인, 참여권 고지, 확인서 작성 등에 관하여는 제12조의 규정을 준용한다.'라고 명시하여 임의제출용 전자정보 확인서의 간이서식 신설 및 해시값 생성, 참여권 보장 등 디지털 증거의 압수방법을 준용하도록 규정하였다.

2.3 피압수자 참여권 보장에 따른 문제점

하지만 피압수자 참여권 보장의 헌법적 가치에도 불구하고, 수사기관에서는 부작용에 대한 우려와 함께 비효율성에 대한 불만이 높아지고

있는 실정이다. 피압수자 참여권 보장에 따른 대표적인 문제점들은 다음과 같다.

첫 번째로는 신속성 저하이다. 수사기관이 사건을 진행할 때 가장 중요하게 생각하는 것은 보안과 신속성이다. 따라서 분석관은 피의자의 범죄혐의를 입증할 만한 단서를 빠른 시간 안에 수사관에게 제공하기 위하여 업무 외 시간인 야간, 주말에도 근무하고 있다. 하지만 수사기관에서 유관정보의 탐색・출력・복제 행위를 피압수자 측의 참여 없이 진행할 경우 원칙적으로 위법이 되기 때문에, 피압수자 측에서 이러한 참여권 보장을 악용하여 참여 일정을 연기하거나, 야간・주말 분석에 대한 참여 반대, 참여 일정을 압수일자가 많이 경과된 일정으로 잡는 등으로 수사를 방해한다면, 해당 증거물에 대한 분석 작업이 지연되어 수사의 신속성을 저하시킬 수 있다.

둘째로는 보안 문제와 분석기법 노출 우려이다. 피압수자 측의 참여는 짧게는 반나절, 길게는 한 달 동안 이어질 수 있다. 수사기관 사무실에 별도의 참여실이 갖춰지지 않았을 경우, 사무실 내에서 참여를 진행하게 되는데 이 과정에서 참여인은 사무실 내에서 분석관과 수사관의 대화내용 및 분위기, 전화통화, 분석관들의 분석기법 대화 등을 듣게 될 우려가 있다. 또한, 분석관 책상 위나 주변에서 사건관련 자료를 볼 수 있는 경우도 발생할 수 있다. 별도의 참여실이 있더라도, 대부분의 참여실 안에 분석관과 참여인 간의 독립적인 공간이 마련되어 있지 않기 때문에 참여인은 분석관의 옆자리 또는 뒷자리에서 분석관의 모니터를 지켜보며 감시하게 된다. 분석관은 디지털 증거의 특성인 비가시성, 비가독성을 특정 프로그램을 사용하여 읽을 수 있는 상태로 전환한 후, 디지털 증거에 대하여 삭제 데이터 영역 복구, 은닉정보 변환, 암호파일의 해독 등의 기술적 조치를 취하게 되는데 만약 IT 지식이 있는 참여인일 경우, 분석 및 탐색과정을 지켜볼 때 특정 분석기법이 유출될 수 있다.

세 번째로는 증거인멸의 우려이다. 수사기관의 분석실에는 증거물에 대한 무결성을 유지하기 위하여 전파차단시설을 갖추고 있는 획득실에 증거물을 보관하고 이미지를 획득한다. 2016년부터 각 지방청에 순차적으로 참여실을 설치하고 있으나, 참여실이 설치되지 않은 수사기관 사무실에서는 전파차단시설이 없는 장소에서 참여를 진행하게 된다. 특정 스마트폰 모델의 경우, 이미지 획득을 위해 비행기 모드를 해지하여 네트워크에 접속하는데 참여인이 사건관계자와 사전에 모의하여 네트워크에 접속하는 시점을 사건관계자에게 알려줌으로써 원격초기화 또는 킬 스위치(Kill Switch)를 통해 원격 잠금을 하거나 개인정보를 삭제하여 증거인멸이 가능하다.

마지막으로 분석지연의 발생이다. 2017년 기준으로 사이버안전국에 소속되어 있는 디지털 증거분석관의 인력은 총 67명이다. 2016년 총 디지털 증거분석 건수를 전국 디지털 증거분석관 인원으로 나눈 결과, 연 481건으로 나타났다. 디지털 증거분석관의 적정 분석 건수인 연 212건을 훨씬 웃도는 수로 분석인원은 턱없이 부족한 실정이다[8]. 또한, 2015년 경찰청 조사 당시에는 참여권 보장으로 소요되는 시간산정은 제외되어 있었으므로, 만약 참여권 보장으로 인한 소요시간을 산정한다면 적정건수는 연 212건보다 더 줄어야 한다. 따라서 피압수자 참여가 많아지거나 장기간 참여로 이어질 경우, 다른 사건에 대한 분석 지연은 피할 수 없게 된다.

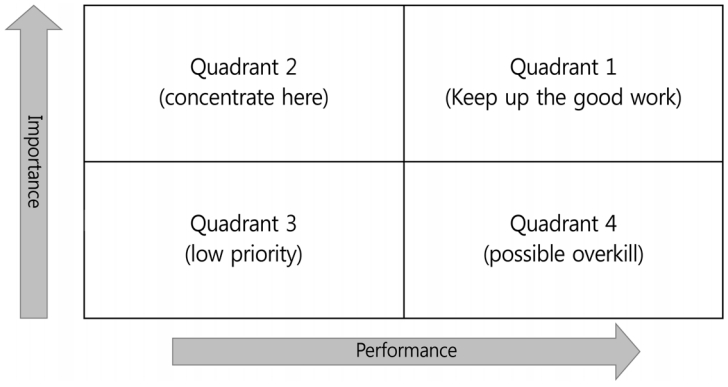
3. 연구방법

3.1 중요도-이행도 분석(IPA)

IPA(Importance Performance Analysis)는 기업 혹은 고객이 각 요인별로 상대적인 중요도와 이행도(만족도)를 동시에 비교하여 분석할 수 있는 평가방법으로서 1970년대 경영학 분야에서 처음 소개되었다[5]. 마케팅, 교육, 관광 등의 여러 분야에서 활용되었으며, 특히 서비스 경영 분야에서 현재 수준을 평가하고 개선점을 찾아내기 위한 방법으로 다양하게 활용되고 있다[3]. IPA를 활용한 평가방법은 분석결과를 4분면에 도식화함으로써 시각적으로 쉽게 이해되며, 어떤 분야에 역량을 집중할 것인지를 명백히 제시해 주는 특징을 가지고 있다. 즉, 다양하고 복잡한 성격을 가진 요인들을 일목요연하게 평가할 수 있으며, 어려운 통계적 기법을 사용하지 않고 중요도와 이행도의 평균값만으로 유용한 결과를 도출해 낼 수 있다. 따라서 정책 결정자뿐만 아니라 실무자들에게도 활용도가 매우 높은 평가기법이라 하겠다.

IPA는 분석대상인 측정문항들을 중요도(Importance)와 이행도(Performance)에 따라, 2×2 매트릭스 상에 표시한다. 평균값을 기준으로 나누어진 4사분면(quadrant)에 <Figure 1>과 같이 각각의 의미를 부여한다.

각 사분면별 특징은 다음과 같다. 첫째, 제1사분면(지속유지: keep up the good work)은 중요도와 이행도가 모두 높은 영역으로, 속성항목에 대하여 중요하게 생각하고 있고, 실제 속성항목에 대한 이행도 잘 되고 있는 상태로 지속적으로 유지해 나가는 것이 좋다. 둘째, 제2사분면(중점개선: concentrate here)은 중요도는 높으나 이행도가 낮은 영역으로, 속성항목에 대하여 중요하게는 생각하고 있으나, 실제로는 잘 이행되고 있지 않은 상태로 집중하여 개선하는 것이 좋다. 셋째, 제3사분면(점진개선: low priority)은 중요도와 이행도가 모두 낮은 영역으로, 속성항목에 대하여 중요하게 생각하지 않고, 실제 속성항목에 대하여 이행도 잘 되고 있지 않은 상태로 의사결정에 큰 영향을 미치지 않는 영역이다. 넷째, 제4사분면(과잉: possible overkill)은 중요도는 낮으나 이행도가 높은 영역으로, 이행노력을 감소하거나 상황에 따라 중단할 필요성이 있다. 하지만, 높은 이행도가 적은 노력에 의해서 이루어진 것이라면 지속적으로 유지해도 무방하다[3, 5].



〈Figure 1〉 Importance-Performance Matrix(Recited from[Martilla and James, 1977])

3.2 연구의 절차

본 연구의 절차는 다음과 같다. (1)상위 영역 개발 및 측정항목 도출, (2)측정항목 정제 및 수정, (3)측정항목 검증을 거쳐서, 최종 측정항목을 개발하였다. 마지막으로, (4)도출된 측정항목을 활용하여 중요도와 이행도에 대한 설문조사를 실시하였다. 현장 외 반출된 정보저장매체의 참여권 보장 환경을 측정하는 항목에 대한 선행연구가 거의 존재하지 않으므로, 관련 법규와 훈령을 검토하고 세 차례의 전문가 인터뷰를 실시하였다. 각 환경을 측정하는 상위 영역을 절차, 장소, 사람, 기술의 네 가지로 설정하고, 하위 측정항목을 도출하고 타당성을 검증하였다. 전문가 그룹은 사이버수사 또는 민간 경력 최소 3년 이상의 포렌식 전문가 12인

〈Table 2〉 Dimensions and Measurement Items

Dimension	Measurement Item
Process	1. Make a participation confirmation after notifying the participation right
	2. Explain to participants the process of seizure of digital evidence
	3. Select available days for participation by coordinating the schedule of participant, investigator, and analyst
	4. Preliminary meeting to share case information before participation
	5. Check for the latest version of analytical equipment, programs, etc. before participation
	6. Limit the communication media of the participant to prevent evidence destruction
	7. Seize materials only related to criminal charges
	8. Provide detailed list(including hash value) of selection, output, duplicated data from digital evidence to participant
	9. Completion of revocation
	10. Make a receipt when returning digital storage media
	11. Provide standard guidelines(guidelines) on procedures and methods for ensuring participation for investigator and analyst
	12. Store documents related to participation separately
Location	13. Sufficient size of rooms capable of accommodating the participants
	14. Make resting space in the participating room for long time participation
	15. Separate space for participant and analyst
	16. Prepare facility to prevent breach of analytic technique
	17. Install a lock on the place of participation in case you need to suspend participation
	18. Equip CCTV to demonstrate the integrity of the participating process
	19. Equip radio wave interception facility to ensure the integrity of digital evidence at participating locations
People	20. Participant's understanding the definition, procedure, and scope of ensuring participation
	21. Voluntary involvement of participants
	22. Proper use of participant's right(Do not interfere investigation, Do not abuse it for personal benefit)
	23. Recognize participant's right accurately(definition, procedure, scope, etc.)
	24. Acknowledge the subjective role of investigator in ensuring participant's right
	25. Select an analyst capable of use of scientific techniques, equipment and programs
Techno-logy	26. Acquire images using a write-protect device for digital evidence integrity
	27. Confirm participants to analyze the same image as the acquired image(check the hash value)
	28. Describe the equipment and programs used in the participation process(acquisition, analysis, screening, output) to the participant
	29. Explain terminology to help participant's understanding
	30. Describe techniques used to acquire and analyze digital evidence for participants

으로 구성하였다. 1차 전문가 인터뷰에서는 상위 영역의 종류와 조작적 정의를 확정하고, 2차 인터뷰에서는 상위 영역의 내용타당성을 검증하고 측정항목의 조작적 정의를 확정하였다. 최종적으로 3차 전문가 인터뷰를 통해 도출된 측정항목의 내용타당성을 검증하였다. 참여권 보장 환경은 절차 12문항, 장소 7문항, 사람 6문항, 기술 5문항으로 중요도와 이행도 각 30문항씩으로, 총 60개의 문항으로 구성되어 있다. 그 외 인구 통계학적 특성에 관한 항목 16개를 포함하여 총 76개 문항으로 구성되었다. 설문의 상위 개념과 하위 측정문항은 <Table 2>와 같다.

IPA 분석을 위하여, 전국의 디지털 증거분석관 58명을 대상으로 2017년 11월 16일부터 11월 20일까지 온라인 설문을 실시하였다. 설문은 무기명이며 학술적 용도로만 사용된다는 점을 강조하여 연구대상자들이 솔직하게 의견을 표현할 수 있도록 하였다. 자료 분석을 위해 SPSS 25.0과 MS-Excel 2010을 활용하였다. SPSS 25.0 통계프로그램을 활용하여, 참여권 보장 환경에 대한 중요도와 이행도의 차이를 t-test로 검정하였고, MS-Excel 2010을 활용하여 빈도분석 및 IPA 매트릭스 분석을 실시하였다.

4. 연구의 결과

4.1 응답자 특성 및 사전 조사 결과

본 연구의 응답자는 경찰청 및 지방경찰청에서 근무하고 있는 디지털 증거분석관이기 때문에 자세한 응답자 특성은 공개할 수 없으며, 대략의 인구통계학적 특성은 다음과 같다. 소속기능으로는 사이버기능이 52명(89.7%), 보안기능 5명(8.6%), 기타 1명(1.7%)으로 나타났다. 경찰 및 타 기관, 민간 업계의 경력을 포함한 디지털 포렌식 경력은 1년 이상 3년 미만이 25명(43.1%), 3년 이상 5년 미만이 19명(32.8%), 5년 이상 7년 미만이 6명(10.3%), 1년 미만이 3명(5.2%)으로, 3년 이상 5년 미만의 포렌식 경력이 가장 많았다. 성별은 남자가 47명(81%)으로 여자 11명(19%)보다 많은 경향을 보였다. 참여권 보장 환경에 대한 전반적인 상황을 조사하기 위해 두 가지 사전 조사를 실시하였으며 결과는 다음과 같다.

첫째, 현장 외 반출된 정보저장매체의 증거탐색에 평균적으로 참여하는 인원은 3명 이하 35명(60.3%), 4명 이상 5명 이하 17명(29.3%), 6명 이상 7명 이하 4명(6.9%), 10명 이상 2명(3.4%) 순으로 나타났다. 분석의뢰물의 소유자, 사용자 또는 대리인인 참여인 1명, 사건 담당 수사관 1명, 분석의뢰물 담당 증거분석관 1명이 참여하여 분석하는 것이 일반적이므로 3명이 참여하는 경우가 가장 많았다.

둘째, 참여 하에 디지털 증거분석을 수행할 경우에 참여 없이 진행할 경우보다 시간이 얼마나 더 소요되는지를 설문한 결과이다. 시간 단위로 작성하지 않고 비율(%)이나 배수로 응답하거나 무응답한 경우는 제외하였다. 조사결과 사건 한 건 당 평균 26시간이 더 소요되는 것으로 나타났다. 참여인과 수사관, 분석관의 참여 일정 조율부터, 분석 장비와 프로그램에 대한 점검 시간, 참여인이 휴식을 원할 경우 대기시간, 수사관 또는 분석관이 분석결과에 대해 사건 관련 자료여부를 확인 및 선별 할 때 참여인의 확인 작업 등으로 인해 추가 발생하는 시간 등으로 나타났다.

4.2 수사기관의 참여권 환경 항목의 중요도와 이행도 차이

수사기관의 분석관들이 참여권 보장 환경에서 각 항목별로 중요하게 생각하는 정도와 현재 이행되고 있는 수준의 차이를 살펴보기 위하여, 대응표본 t-test를 활용하여 분석하였다.

<Table 3>는 중요도를 기준으로 총 30개의 항목을 가장 높은 평균값 순서대로 나열한 후, 중요도와 이행동의 평균값에 유의미한 차이가 있는지를 검증한 결과이다. 대부분의 항목에서 중요도와 이행도의 순위와 평균값에서 유의미한 차이를 보였다. 특히 중요도 1위인 '참여권 보장의 주체적 역할인지'는 이행도에서는 낮은 수준(19위)을 보이고 있었다. 또한 평균값의 유의미한 차이가 있는 모든 항목에서 중요도의 수준이 이행도보다 높은 것을 볼 때, 참여권 보장 환경에 있어 많은 개선이 요구되는 것으로 보인다.

〈Table 3〉 Comparison of Importance and Performance Level

Measurement Items	Importance			Performance			t-value	p-value
	Mean	STD	Rank	Mean	STD	Rank		
24. Subjective role of investigator	6.41	1.33	1	4.86	1.64	19	6.07***	0.00
23. Recognition of participation right	6.33	1.29	2	5.41	1.38	10	5.78***	0.00
26. Image Acquision	6.21	1.46	3	6.40	1.35	1	-1.18	0.24
22. Proper use of participant's right	6.19	1.42	4	4.48	1.70	23	6.36***	0.00
27. Checking hash value	6.17	1.57	5	6.16	1.57	2	0.10	0.92
25. Selection of analyst	6.16	1.40	6	5.93	1.62	4	1.12	0.27
1. Parcipation confirmation	6.14	1.59	7	5.86	1.40	5	1.29	0.20
11. Standard policy	6.07	1.43	8	5.16	1.95	13	3.33***	0.00
16. Facility to prevent breach	6.05	1.41	9	3.40	2.11	28	7.84***	0.00
18. CCTV	6.05	1.66	10	6.12	1.80	3	-0.24	0.82
5. Checking analytic tool	6.03	1.44	11	5.66	1.62	7	1.71	0.09
9. Revocation	6.02	1.46	12	5.57	1.73	9	2.37*	0.02
6. Restriction of communication media	5.97	1.52	13	3.81	2.15	27	7.07***	0.00
8. Distribution of detailed list	5.95	1.58	14	5.59	1.57	8	1.91	0.06
21. Voluntary involvement	5.93	1.47	15	5.34	1.45	11	2.68*	0.01
2. Explanation of process	5.84	1.50	16	5.19	1.37	12	3.40***	0.00
3. Coordination of participation schedule	5.84	1.50	17	5.76	1.48	6	0.40	0.69
13. Sufficient Room for participation	5.84	1.52	18	4.81	2.04	20	3.20***	0.00
10. Receipt for return	5.83	1.44	19	5.16	1.84	13	2.70**	0.01
15. Separation of space	5.83	1.75	20	4.22	2.39	24	4.53***	0.00
17. Installation of a lock	5.83	1.63	21	5.00	2.18	16	2.54*	0.01
20. Participant's understanding of participation right	5.76	1.36	22	4.53	1.55	22	5.16***	0.00
7. Seizure of crime-related material only	5.45	1.75	23	5.00	1.76	16	1.48	0.15
4. Preliminary meeting	5.36	1.65	24	4.00	1.94	26	4.19***	0.00
19. Radio wave interception facility	5.33	1.79	25	2.97	2.30	29	6.80***	0.00
12. Separation of document	5.22	2.01	26	5.03	1.86	15	0.76	0.45
29. Explanation of terminology	4.71	1.52	27	4.57	1.50	21	0.77	0.45
28. Explanation of program	4.55	1.62	28	4.91	1.44	18	-1.91	0.06
14. Resting place	4.33	1.82	29	2.78	1.86	30	4.66***	0.00
30. Description of technique	4.10	1.73	30	4.03	1.72	25	0.39	0.70

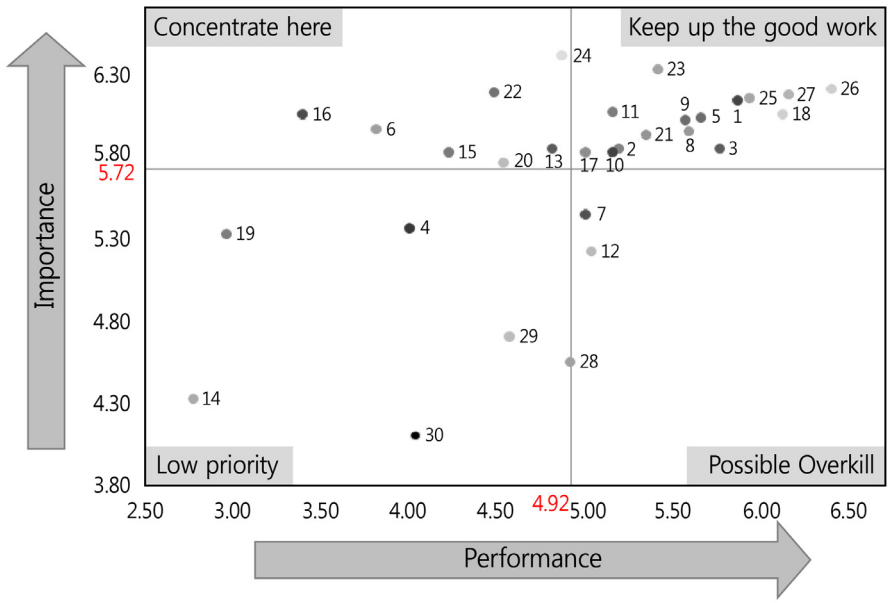
*p < 0.05, **p < 0.01, ***p < 0.001.

4.3 수사기관의 참여권 보장 환경에 대한 IPA 매트릭스 분석

수사기관의 분석관들이 인지하고 있는 참여권 보장 환경에 대한 IPA 매트릭스 분석 결과는 <Figure 2>와 <Table 4>와 같다. X축은 이행도를 나타내며 평균값은 4.92이고, Y축은 중요도를 의미하며 평균값은 5.72로 각 축의 기준교점으로 설정되었다. 전체 항목 중 '참여권 보장의 주체적 역할인지'는 가장 높은 중요도를, '이미지 획득의 신뢰성 보장'은 가장 높은 이행도를 나타내고 있으며, '분석기술 설명'이 가장 낮은 중요도로, '휴식 공간'이 가장 낮은 이행도로 나타났다.

〈Table 4〉 Allocated Items by IPA Dimensions

Keep up the good work (15 items)	1. Make a participation confirmation after notifying the participation right 2. Explain to participants the process of seizure of digital evidence 3. Select available days for participation by coordinating the schedule of participant, investigator, and analyst 5. Check for the latest version of analytical equipment, programs, etc. before participation 8. Provide detailed list(including hash value) of selection, output, duplicated data from digital evidence to participant 9. Completion of revocation 10. Make a receipt when returning digital storage media 11. Provide standard guidelines(guidelines) on procedures and methods for ensuring participation for investigator and analyst 17. Install a lock on the place of participation in case you need to suspend participation 18. Equip CCTV to demonstrate the integrity of the participating process 21. Voluntary involvement of participants 23. Recognize participant's right accurately(definition, procedure, scope, etc.) 25. Select an analyst capable of use of scientific techniques, equipment and programs 26. Get images using a write-protect device for digital evidence integrity 27. Confirm participants to analyze the same image as the acquired image(check the hash value)
Concentrate here (7 items)	6. Limit the communication media of the participant to prevent evidence destruction 13. Sufficient size of rooms capable of accommodating the participants 15. Separate space for participant and analyst 16. Prepare facility to prevent breach of analytic technique 20. Participant's understanding the definition, procedure, and scope of ensuring participation 22. Proper use of participant's right(Do not interfere investigation, Do not abuse it for personal benefit) 24. Acknowledge the subjective role of investigator in ensuring participant's right
Low priority (6 items)	4. Preliminary meeting to share case information before participation 14. Make resting space in the participating room for long time participation 19. Equip radio wave interception facility to ensure the integrity of digital evidence at participating locations 28. Describe the equipment and programs used in the participation process(acquisition, analysis, screening, output) to the participant 29. Explain terminology to help participant's understanding 30. Describe techniques used to acquire and analyze digital evidence for participants
Possible overkill (2 items)	7. Seize materials only related to criminal charges 12. Store documents related to participation separately



〈Figure 2〉 IPA Matrix

첫째, 지속유지영역(1사분면)은 수사기관의 분석관들이 참여권 보장 환경에서 중요하다고 생각하며 이행도 역시 높은 요인이라 할 수 있다. 1사분면에 해당하는 항목으로는 '참여권 고지 후 참여확인서를 작성', '참여인에게 디지털 증거의 압수절차를 이해할 수 있게 설명', '참여인·수사관·분석관의 일정을 조율하여 참여일 선정', '참여 전에 분석장비와 프로그램 등의 최신 버전 및 이상 유무를 점검', '디지털 증거에서 선별·출력·복제한 자료의 상세목록(해시값 포함)을 참여인에게 교부', '참여 철회 시 참여철회 확인서 작성', '디지털 저장매체 원본 반환 시 인수증 작성', '수사관·분석관을 위한 참여권 보장 절차 및 방법 등에 대한 표준 지침(가이드라인)을 제공', '참여를 일시 중단하는 경우를 대비하여 참여장소에 잠금장치 설치', '참여과정의 무결성 입증을 위해 CCTV 설비', '참여인은 타인의 의사가 아닌 자발적 의사로 참여', '수사기관의 참여권 보장의 정의·절차·범위 등을 숙지', '과학적 기법과 장비 및 프로그램 등의 사용이 가능한 증거분석관을 선정', '디지털 증거 무결성을 위해 쓰기방지장치 등을 사용하여 이미지를 획득', '획득한 이미지와 동일한 이미지로 분석하는 것을 참여인에게 확인(해시값 확인)'으로 총 30개 항목 중 15개 항목이 이에 해당되었다. 이와 같이 15개 항목은 분석관들이 중요하다고 생각함과 동시에 잘 이행하고 있으므로 계속 유지해 가는 전략이 필요하다.

둘째, 중점개선영역(2사분면)은 수사기관의 분석관들이 참여권 보장 환경에서 중요하다고 생각하지만, 낮은 이행도를 보이는 속성을 의미한다. 해당 항목으로는 '증거인멸 방지를 위해 참여인의 통신매체를 제한', '참여인원을 수용할 수 있는 규모의 참여실', '참여인 공간과 분석관 공간의 분리', '분석기법 유출에 대비한 시설', '참여인의 참여권보장(정의, 절차, 범위 등)에

대한 정확한 인지', '참여인의 올바른 참여권 사용(수사방행, 개인적 이익을 위한 사용 금지)', '참여권 보장의 주체적 역할이 사건 담당 수사관임을 인지'의 7개 항목이 이에 해당된다. 이와 같이 2사분면은 분석관들이 중요하게 생각하지만 이행도 수준이 낮기 때문에 이를 극복하기 위한 개선과 지원이 적극 요구되는 사항들이다.

셋째, 점진개선영역(3사분면)은 수사기관의 분석관들이 인지하는 중요도와 이행도가 모두 낮은 영역으로, 본 연구에서는 전체 30개 항목 중에서 6개가 이에 속한다. '참여 전 사건 정보 공유를 위한 사전 정보 회의', '장시간 참여를 고려하여 참여실에 휴식공간 마련', '디지털 증거의 무결성 보장을 위한 전파차단 시설', '참여인에게 참여과정(획득, 분석, 선별, 출력)에서 사용되는 장비와 프로그램을 설명', '참여인에게 디지털 증거 획득 및 분석에 사용된 기술 설명'이 여기에 속한다.

넷째, 과잉영역(4사분면)은 중요도는 낮게 인식하고 있으나, 이행도는 높은 수준을 보이는 항목을 의미하며, 본 연구에서는 '범죄혐의 사실과 관련된 자료만 압수', '참여권과 관련된 서류를 별도 보관'이 이에 포함되었다.

5. 결 론

5.1 연구결과 요약 및 시사점

본 연구는 대법원 2015. 7. 16자 2011모 1839 전원합의체 결정에서 정보저장매체 등의 압수수색 절차에서 피압수자의 참여권 보장의 중요성을 강조함에 따라, 정보저장매체 반출 및 디지털 증거탐색 과정에서의 참여권 보장 환경에 대한 중요도와 이행도를 알아보고, 우선적으로 개선 및 보완할 영역을 파악하는 데 목적이 있다. 이를 위해 수사기관의 증거분석관을 대상으로 4개 상위 개념에 따른 30개 하위 측정항목의 설문조사를 시행하여 중요도와 이행도를 비교 분석하였다. 본 연구의 결과를 요약하면 다음과 같다.

첫째, 수사기관의 참여권 보장 환경에 대해 4개 상위 영역 중요도와 이행도를 IPA 매트릭스로 살펴본 결과, 지속유지영역은 사람과 절차, 점진개선영역은 장소, 과잉영역은 기술로 나타났다. 상위 영역의 중요도와 이행도의 평균값의 차를 살펴본 결과, 기술을 제외한 나머지 절차, 장소, 사람은 중요도가 이행도보다 높게 나타났으며, 중요도와 이행도의 평균값의 차이는 장소(1.42점), 사람(1.03점), 절차(0.66점), 기술(-0.06점) 순으로 나타났다. IPA 매트릭스 결과와 중요도와 이행도의 평균값 차이를 비교한 결과, 중요도가 높은 요인은 지속유지영역에 나타났으며 이행도가 높은 항목은 과잉영역으로 일관성 있게 나타났다. 그러나 장소는 예외적으로 중요도는 높으나 IPA 매트릭스 결과는 점진개선영역으로 표현되었다. 이는 장소영역의 중요도와 이행도의 평균값의 차이가 상위 4개요인 중 가장 크며, <Table 2>에서 나타나듯이, 중요도와 이행도의 평균값 차이가 높은 상위 5개 항목에서 '분석기법 유출 대비 시설', '전파차단 시설', '참여인과 분석관의 공간 분리'의 3개의 항목이 장소요인으로 나타난 것으로 보아, 중요도 대비 시설과 같은 제반사항이 뒷받침 되지 않아 이행도가 낮게 나타난 것으로 보인다.

둘째, 수사기관의 참여권 환경의 중요도와 이행도 간의 항목별 차이를 살펴본 결과, 중점개선영역에 속한 7개 항목은 절차 항목 1개(#6), 장소 항목 3개(#13, #15, #16), 사람 항목 3개

(#20, #22, #24)로 나타났다. 과잉영역으로는 2개 항목 모두 절차요인의 항목으로 '범죄 혐의 사실과 관련된 자료만 압수', '참여권관 관련된 서류의 별도 보관'이 중요도보다 이행도가 높게 나타났다. 판례에서 제시하는 참여권 보장 목적인 프라이버시 침해의 최소화에 해당하는 항목인 '범죄혐의사실과 관련된 자료만 압수'는 과잉영역에, '디지털 증거에서 선별・출력・복제한 자료의 상세목록(해시값 포함)을 참여인에게 교부'는 지속유지영역에 포함되어 있어, 절차는 참여권 보장 목적에 맞게 잘 이행되고 있는 것으로 보인다.

4개 상위 영역의 IPA 매트릭스 결과를 중점개선영역 중심으로 분석해 보면 다음과 같다. 먼저 절차에 있어서 IPA 매트릭스 상 중점개선영역은 '증거인멸방지를 위해 참여인의 통신매체제한'으로 나타났다. 이를 우선적으로 보완하여, 참여인이 사건관계자와 사전에 모의하여 개인정보를 삭제하여 증거인멸이 가능한 점을 철저히 방지해야 할 것이다.

다음으로 장소의 중점개선영역은 '분석기법 유출 대비 시설'로 나타났다. 실제 참여 환경을 살펴보면 참여실이 마련되어 있더라도 대부분 참여인과 분석관의 공간이 별도로 존재 하지 않아, 참여인은 분석관의 옆자리 또는 뒷자리에 착석하여 분석과정을 지켜보게 된다. 이 과정에서 IT 지식, 특히 포렌식 관련 지식이 있는 참여인일 경우 분석과정을 모두 지켜보게 되므로 데이터 복구, 데이터 검색, 은닉 데이터 탐지 등의 분석기법이 유출 될 수 있다. 또한, 참여실이 별도로 존재하지 않는 경우에는 분석실에 상주하게 되어, 분석관들 간의 분석기법 및 분석내용 논의, 사건 관련 대화내용 등을 접할 수 있게 되어 분석기법 유출 뿐 아니라 수사의 기밀성과 보안성이 제대로 지켜지지 않게 된다. 사전조사 결과, 증거 탐색 과정에 참여하는 평균 인원은 3명 이하가 60.3%로 가장 많은 비중을 차지하고 있으나, 10명 이상도 3.4%로 나타났다. 향후 이를 근거로 참여실 설계 기준을 예규로 제정하거나 신규 참여실을 마련하는 관서에서는 해당 항목들을 고려하여 그에 준하는 공간, 시설을 갖추는 것이 필요하다.

다음으로 사람 영역의 IPA 매트릭스에서 중점개선사항은 '참여인의 올바른 참여권 사용(수사방해, 개인적 이익을 위한 사용 금지)', '참여권 보장의 주체적 역할에 대한 담당 수사관의 인지'로 나타났으며, 두 항목 모두 중요도와 이행도의 평균값의 차이가 매우 높게 나타났다. 압수수색 시 주체적 역할을 하는 담당 수사관은 참여 단계 역시 압수수색 단계에 포함됨을 인지하여 참여 과정을 분석관에게 일임하기 보다는 좀 더 주도적, 적극적으로 참여하는 것이 필요하다. 또한 '참여인의 올바른 참여권 사용'을 유도하기 위해서는 수사를 지연시킬 목적, 유치장에 있기 싫다는 등의 부당한 사유로 참여권 보장을 악용하는 사례를 방지하기 위한 제도적 장치가 필요하다.

마지막으로 기술에 있어서는 중점개선영역이 없고, 지속유지와 점진개선영역만 나타난 것을 볼 때, 다른 영역에 비해 상대적으로 급하게 개선해야 하는 사항은 없는 것으로 보인다.

5.2 연구의 한계점 및 향후 연구과제

본 연구는 현장 외 반출된 정보저장매체에 대한 수사기관의 참여권 보장 환경의 중요도와 이행도를 측정 및 분석하였는데, 연구의 한계점은 다음과 같다.

첫째, 본 연구는 현장 외 반출 된 정보저장매체에 대한 수사기관의 참여권 보장 환경의 중요도와 이행도를 측정하는데 수사관을 제외한 분석관만을 선정하여 연구의 결과를 도출하였다. 따라서 본 연구결과를 수사기관의 입장으로 일반화를 시키기에는 한계가 있다.

둘째, 참여권 보장의 주체인 참여인(피압수자, 참고인, 대리인, 변호인)에 대한 직접적인 조사를 수행하지 못하였다. 향후 수사기관과 참여인의 인식 차이에 대한 연구가 이루어진다면 더 시의적절한 시사점을 제공할 수 있을 것이다.

이러한 한계점에도 불구하고 본 연구는 경찰청의 규칙 외에는 참여권 보장 환경에 대한 구체적인 지침이 없는 상황에서 현재 수사기관의 분석관이 인식하고 있는 정보저장매체 반출 및 디지털 증거탐색 과정에서의 참여권 보장 환경에 대한 중요도와 이행도를 살펴봄에 따라, 향후 참여권 보장을 위해 수사기관에서 갖추어야 할 제반사항, 제도, 정책 수립에도 유용한 근거로 활용될 수 있을 것으로 기대한다.

References

[1] Choi, H. S. and Lee, S. J., “A Study on the Participation Problem and Computer Image Recording System in the Digital Evidence Search,” Journal of Digital Forensics, Vol. 11, No. 2, pp. 73-92, 2017.

[2] Criminal Procedure Law, http://www.law.go.kr/lsInfoP.do?lsiSeq=179019&efYd=20180107#0000(형사소송법).

[3] Kim, J. S., Kang, S. U., and Lim, G. G., “A Study on the Gap Analysis between Expectation and Perceptions of Users for IPTV Services based on N-Screen Technology,” The Journal of Society for e-Business Studies, Vol. 18, No. 2, pp. 205-222, 2013.

[4] Lee, S. H., “The Target and the End Point of the Seizure and Search of Digital evidence,” Law Review, Vol. 58, No. 4, pp. 33-60, 2017.

[5] Martilla, J. A. and James, J. C., “Importance-Performance Analysis,” Journal of Marketing, Vol. 41, No. 1, pp. 77-79, 1977.

[6] National Police Agency Instruction, https://www.police.go.kr/portal/bbs/list.do?bbsId=B0000032&menuNo=200629(경찰청훈령 디지털증거수집및처리등에관한규칙(제845호, 2017. 8. 28, 일부개정).

[7] Park, B. J., Cha, S. J., and Lee, K. C., “Extension of the Long-term Archival Information Package for Electronic Records to Accommodate Web Records,” The Journal of Society for e-Business Studies, Vol. 15, No. 4, pp. 33-47, 2010.

[8] Yun, H. J., Lee, S. Y., and Lee, C. C., “Deriving Priorities of Competences Required for Digital Forensic Experts using AHP,” The Journal of Society for e-Business Studies, Vol. 22, No. 1, pp. 107-122, 2017.

저 자 소 개

양상희 (E-mail: cyberyang@police.go.kr)
2018년 연세대학교 정보대학원 (디지털포렌식 석사)
2015년~현재 경찰청 디지털포렌식센터
관심분야 디지털포렌식, 정보보호

이중정 (E-mail: cclee@yonsei.ac.kr)
1993년 University of South Carolina MIS (경영학박사)
1993년~2000년 Salisbury State University 부교수
2000년~현재 연세대학교 정보대학원 교수
관심분야 IT performance, IT evaluation measurement, Information Orientation

윤혜정 (E-mail: yunhj@ewha.ac.kr)
2013년 연세대학교 정보대학원 (정보시스템박사)
2013년~2014년 미국 American University 박사 후 연구원
2014년~2016년 연세대학교 정보대학원 연구교수
2016년~현재 이화여자대학교 신산업융학대학 국제사무학과 조교수
관심분야 ICT융합서비스, 정보보호, 스마트워크